



For Home

For Enterprise



Decyphering the Noise Around 'Meltdown' and 'Spectre'



Consumer

Enterprise

Corporate

Authors

Subscribe



Search Blogs

[Home](#) / [Other Blogs](#) / [McAfee Labs](#) / [Decyphering the Noise Around Meltdown and Spectre](#)By **McAfee** on Jan 04, 2018

The McAfee Advanced Threat Research (ATR) Team has closely followed the attack techniques that have been named **Meltdown** and **Spectre** throughout the lead-up to their announcement on January 3. In this post, McAfee ATR offers a simple and concise overview of these issues, to separate fact from fiction, and to provide insight into McAfee's capabilities and approach to detection and prevention.

There has been considerable speculation in the press and on social media about the impact of these two new techniques, including which processors and operating systems are affected. The speculation has been based upon published changes to the Linux kernel. McAfee ATR did

not want to add to any confusion until we could provide our customers and the general public solid technical analysis.

A fully comprehensive writeup comes from Google Project Zero in this informative [technical blog](#), which allowed ATR to validate our conclusions. For more on McAfee product compatibility, see this business [Knowledge Center article](#) and this [Consumer Support article](#).

The Techniques

Meltdown and Spectre are new techniques that build upon previous work, such as “KASLR” and other papers that discuss practical side-channel attacks. The current disclosures build upon such side-channel attacks through the innovative use of speculative execution.

Speculative execution has been a feature of processors for at least a decade. Branch speculation is built on the [Tomasulo algorithm](#). In essence, when a branch in execution depends upon a runtime condition, modern processors make a “guess” to potentially save time. This speculatively executed branch proceeds by employing a guess of the value of the condition upon which the branch must depend. That guess is typically based upon the last step of the same branch’s previous execution. The conditional value is cached for reuse in case that particular branch is taken again. There is no loss of computing time if the condition arrives at a new value because the processor must in any event wait for the value’s computation. Invalid speculative executions are thrown away. The fact that invalid speculations are tossed is a key attribute exploited by Meltdown and Spectre.

Despite the clearing of invalid speculative execution results without affecting memory or CPU registers, data from the execution may be retained in the processor caches. The retaining of invalid execution data is one of the properties of modern CPUs upon which Meltdown and Spectre depend. More information about the techniques is available on the site <https://meltdownattack.com>.

Because these techniques can be applied (with variation) to most modern operating systems (Windows, Linux, Android, iOS, MacOS, FreeBSD, etc.), you may ask, “How dangerous are these?” “What steps should an organization take?” and “How about individuals?” The following risk analysis is based upon what McAfee currently understands about Meltdown and Spectre.

There is already considerable activity in the security research community on these techniques. Sample code for two of the three variants was posted by the Graz University (in an appendix of the [Spectre paper](#)). Erik Bosman has also [tweeted that he has built an exploit](#), though this code is not yet public. An earlier example of side-channel exploitation based upon memory caches was posted to GitHub in 2016 by one Meltdown-Spectre researcher Daniel Gruss. Despite these details, as of this writing no known exploits have yet been seen in the wild. McAfee ATR will continue to monitor researchers' and attackers' interest in these techniques and provide updates accordingly. Given the attack surface of nearly every modern computing system and the relative ease of exploitation, it is highly likely that at least one of the aforementioned variants will be weaponized very quickly.

McAfee researchers quickly compiled the public exploit code for Spectre and confirmed its efficacy across a number of operating systems, including Windows, Linux, and MacOS.

Weaponization

To assess the potential impact of any vulnerability or attack technique, we must first consider its value to attackers. These exploits are uniquely attractive to malicious groups or persons because the attack surface is nearly unprecedented, the attack vector is relatively new, and the impacts (privilege escalation and leaks of highly sensitive memory) are detrimental. The only naturally mitigating factor is that these exploits require local code execution. A number of third parties have already identified JavaScript as an applicable delivery point, meaning both attacks could theoretically be run from inside a browser, effectively opening an avenue of remote delivery. As always, JavaScript is a double-edged sword, offering a more user-friendly browsing experience, but also offering attackers an increased attack surface in the context of the browser's executing scripted code.

Any technique that allows an attacker to cross virtual machine boundaries is of particular interest, because such a technique might allow an adversary to use a cloud virtual machine instance to attack other tenants of the cloud. Spectre is designed to foster attacks across application boundaries and hence applies directly to this problem. Thus, major cloud vendors have rushed to issue patches and software updates in advance of the public disclosure of these issues.

Additionally, both Meltdown and Spectre are exceptionally hard to detect as they do not leave forensic traces or halt program execution. This makes post-infection investigations and attack attribution much more complex.

Recommendations

Because we believe that Meltdown and Spectre may offer real-world adversaries significant value, we must consider how they can be used. There is no remote vector to these techniques; an attacker must first deliver code to the victim. To protect against malicious JavaScript, we always urge caution when browsing the Internet. Allow scripting languages to execute only from trusted sites. McAfee Windows Security Suite or McAfee Endpoint Security (ENS) can provide warnings if you visit a known dangerous site. These McAfee products can also provide an alternate script-execution engine that prevents known malicious scripts from executing. As operating systems are changed to mitigate Meltdown and Spectre, organizations and individuals should apply those updates as soon as possible.

Even though we have not seen any malware currently exploiting these techniques, McAfee is currently evaluating opportunities to provide detection within the scope of our products; we expect most solutions to lie within processor and operating system updates. Based on published proofs of concept, we have provided some limited detection under the names OSX/Spectre, Linux/Spectre, and Trojan-Spectre.

Microsoft has released an out-of-cycle patch because of this disclosure:

<https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892>. Due to the nature of any patch or update, we suggest first applying manual updates on noncritical systems, to ensure compatibility with software that involves the potential use of low-level operating system features. McAfee teams are working to ensure compatibility with released patches where applicable.

While the world wonders about the potential impact of today's critical disclosures, we also see a positive message. This was another major security flaw discovered and communicated by the information security community, as opposed to the discovery or leak of "in the wild" attacks. Will this disclosure have negative aspects? Most likely yes, but the overall effect is more global attention to software and hardware security, and a head start for the good guys on developing more robust systems and architectures for secure computing.

About the Author



McAfee

McAfee is the device-to-cloud cybersecurity company. Inspired by the power of working together, McAfee creates business and consumer solutions that make our world a safer place. Take a look at our latest blogs.

[Read more posts from McAfee >](#)

[< Previous Article](#)

[Next Article >](#)

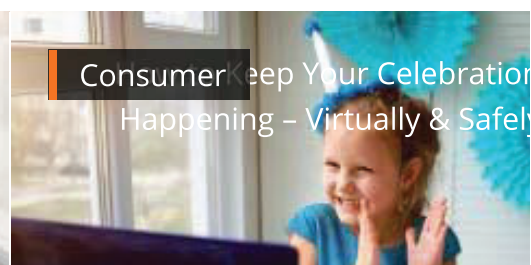
Categories: [McAfee Labs](#)

Tags: [cloud security](#), [computer security](#), [cybersecurity](#), [vulnerability](#), [Advanced Threat Research](#)

Leave a reply


[Facebook Comments](#) [Comments \(0\)](#)

Similar Blogs





Subscribe to McAfee Securing Tomorrow Blogs

 > Securing Tomorrow



 United States / English

[Privacy](#) | [Legal Notices](#) | [Legal Contracts & Terms](#) | [Site Map](#) | Copyright ©2020 McAfee, LLC